BULLETIN (SB20-006)
VULNERABILITY SUMMARY FOR THE WEEK OF DECEMBER 30, 2019

Bulletin (SB20-006)
Vulnerability Summary for the Week of December 30, 2019

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0-6.9 -

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- application_delivery_controller_and_gateway	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	2019-12-27	7.5	CVE-2019-19781 CONFIRM
freeciv -- freeciv	A denial of service flaw was found in the way the server component of Freeciv before 2.3.4 processed certain packets. A remote attacker could send a specially-crafted packet that, when processed would lead to memory exhaustion or excessive CPU consumption.	2019-12-30	7.8	CVE-2012-5645
magnolia_international -- magnolia_cms	Magnolia CMS before 4.5.9 has multiple access bypass vulnerabilities	2019-12-27	7.5	CVE-2013-4621 MISC MISC
open_dynamics -- collabtive	Collabtive 1.0 has incorrect access control	2019-12-27	7.5	CVE-2013-5027 MISC
php-shellcommand -- php-shellcommand	php-shellcommand versions before 1.6.1 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-30	10	CVE-2019-10774 MISC
senkas -- kolibri	Buffer overflow in Senkas Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a POST request.	2019-12-27	7.5	CVE-2014-5289 MISC BID XF
sqlite -- sqlite	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.	2020-01-02	7.5	CVE-2019-20218 MISC
wordpress -- wordpress	wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript: substring.	2019-12-27	7.5	CVE-2019-20041 MISC MISC
yandex -- clickhouse	In all versions of ClickHouse before 19.14, an OOB read, OOB write and integer underflow in decompression algorithms can be used to achieve RCE or DoS via native protocol.	2019-12-30	7.5	CVE-2019-16535 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bolt -- bolt	Bolt 3.6.4 has XSS via the slug, teaser, or title parameter to editcontent/pages, a related issue to CVE-2017-11128 and CVE-2018-19933.	2019-12-31	4.3	CVE-2019-9553 MISC MISC
genjxcms -- genjxcms	GeniXCMS 1.1.5 has XSS via the dbuser or dbhost parameter during step 1 of installation.	2019-12-31	4.3	CVE-2018-14476 MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_SPLINE_private in dwg.spec.	2019-12-27	4.3	CVE-2019-20009 MISC MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.92. There is a use-after-free in resolve_objectref_vector in decode.c.	2019-12-27	6.8	CVE-2019-20010 MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.92. There is a heap-based buffer over-read in decode_R13_R2000 in decode.c.	2019-12-27	6.8	CVE-2019-20011 MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG before 0.93. There is a double-free in dwg_free in free.c.	2019-12-27	6.8	CVE-2019-20014 MISC MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_HATCH_private in dwg.spec.	2019-12-27	4.3	CVE-2019-20012 MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in decode_3dsolid in dwg.spec.	2019-12-27	4.3	CVE-2019-20013 MISC MISC MISC
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_LWPOLYLINE_private in dwg.spec.	2019-12-27	4.3	CVE-2019-20015 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function senc_Parse() in isomedia/box_code_drm.c.	2019-12-31	4.3	CVE-2019-20167 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_odf_avc_cfg_write_bs() in odf/descriptors.c.	2019-12-31	4.3	CVE-2019-20163 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function trak_Read() in isomedia/box_code_base.c.	2019-12-31	4.3	CVE-2019-20169 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function gf_isom_box_dump_ex() in isomedia/box_funcs.c.	2019-12-31	4.3	CVE-2019-20168 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_dump() in isomedia/box_dump.c.	2019-12-31	4.3	CVE-2019-20166 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function ReadGF_IPMPX_WatermarkingInit() in odf/ipmpx_code.c.	2019-12-31	4.3	CVE-2019-20161 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a stack-based buffer overflow in the function av1_parse_tile_group() in media_tools/av_parsers.c.	2019-12-31	4.3	CVE-2019-20160 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function gf_isom_box_parse_ex() in isomedia/box_funcs.c.	2019-12-31	4.3	CVE-2019-20162 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_box_del() in isomedia/box_funcs.c.	2019-12-31	4.3	CVE-2019-20164 MISC
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function ilst_item_Read() in isomedia/box_code_apple.c.	2019-12-31	4.3	CVE-2019-20165 MISC
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 allows overly permissive cross-origin resource sharing which could allow an attacker to transfer private information. An attacker could exploit this vulnerability to access content that should be restricted. IBM X-Force ID: 161422.	2019-12-30	4	CVE-2019-4343 XF CONFIRM
ibm -- mq	IBM MQ 9.1.0.0, 9.1.0.1, 9.1.0.2, 9.1.0.3, 9.1.1, 9.1.2, and 9.1.3 is vulnerable to a denial of service attack that would allow an authenticated	2019-12-30	4	CVE-2019-4655

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user to reset client connections due to an error within the Data Conversion routine. IBM X-Force ID: 170966.			XF CONFIRM
ibm -- watson_studio_local	IBM Watson Studio Local 1.2.3 could disclose sensitive information over the network that an attacked could use in further attacks against the system. IBM X-Force ID: 145238.	2019-12-30	5	CVE-2018-1682 XF CONFIRM
joomla! -- joomla!	Xorbin Analog Flash Clock 1.0 extension for Joomia has XSS	2019-12-27	4.3	CVE-2013-4692 MISC MISC MISC
libsixel_project -- libsixel	A memory leak was discovered in image_buffer_resize in fromsixel.c in libsixel 1.8.4.	2019-12-27	4.3	CVE-2019-20023 MISC
libsixel_project -- libsixel	An invalid memory address dereference was discovered in load_pnm in frompnm.c in libsixel before 1.8.3.	2019-12-27	4.3	CVE-2019-20022 MISC
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_init_frame at fromgif.c.	2019-12-30	6.8	CVE-2019-20094 MISC
libsixel_project -- libsixel	A heap-based buffer overflow was discovered in image_buffer_resize in fromsixel.c in libsixel before 1.8.4.	2019-12-27	4.3	CVE-2019-20024 MISC
livefyre -- livecomments	Cross-site scripting (XSS) vulnerability in Livefyre LiveComments 3.0 allows remote attackers to inject arbitrary web script or HTML via the name of an uploaded picture.	2019-12-27	4.3	CVE-2014-6420 MISC XF
luquidpixels -- liquifire_os	LuquidPixels LiquiFire OS 4.8.0 allows SSRF via the call%3Durl substring followed by a URL in square brackets.	2019-12-29	6.4	CVE-2019-20055 MISC
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi hostname parameter (Dynamic DNS Configuration).	2019-12-30	4.3	CVE-2019-20072 MISC MISC MISC
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi username parameter (DynDns settings of the Dynamic DNS Configuration).	2019-12-30	4.3	CVE-2019-20076 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the urlFQDN parameter to form2url.cgi (aka the Keyword field of the URL Blocking Configuration).	2019-12-30	4.3	CVE-2019-20070 MISC MISC MISC
netis -- dl4323_devices	On Netis DL4323 devices, pingrtt_v6.html has XSS (Ping6 Diagnostic).	2019-12-30	4.3	CVE-2019-20075 MISC MISC MISC
netis -- dl4323_devices	On Netis DL4323 devices, any user role can view sensitive information, such as a user password or the FTP password, via the form2saveConf.cgi page.	2019-12-30	4	CVE-2019-20074 MISC MISC
netis -- dl4323_devices	On Netis DL4323 devices, CSRF exists via form2logaction.cgi to delete all logs.	2019-12-30	5.8	CVE-2019-20071 MISC MISC MISC
netis -- dl4323_device	On Netis DL4323 devices, XSS exists via the form2userconfig.cgi username parameter (User Account Configuration).	2019-12-30	4.3	CVE-2019-20073 MISC MISC MISC
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /search.htm searchtext parameter. NOTE: This product is discontinued.	2019-12-31	4.3	CVE-2019-9207 MISC MISC
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /public/login.htm errormsg or loginurl parameter. NOTE: This product is discontinued.	2019-12-31	4.3	CVE-2019-9206 MISC MISC
pillow -- pillow	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.	2020-01-03	6.8	CVE-2020-5312 MISC MISC
pillow -- pillow	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc.	2020-01-03	6.8	CVE-2020-5310

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
pillow -- pillow	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.	2020-01-03	6.8	CVE-2020-5313 MISC MISC
pillow -- pillow	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow.	2020-01-03	6.8	CVE-2020-5311 MISC MISC
proxyman -- proxyman_for_macos	com.proxyman.NSProxy.HelperTool in Privileged Helper Tool in Proxyman for macOS 1.11.0 and earlier allows an attacker to change the System Proxy and redirect all traffic to an attacker-controlled computer, enabling MITM attacks.	2019-12-29	4.3	CVE-2019-20057 MISC
sencha_labs -- connect	Sencha Labs Connect has XSS with connect.methodOverride()	2019-12-27	4.3	CVE-2013-4691 MISC
spbas -- business_automation_software	SPBAS Business Automation Software 2012 has CSRF.	2019-12-27	4.3	CVE-2013-4665 MISC MISC
spbas-- business_automation_software	SPBAS Business Automation Software 2012 has XSS.	2019-12-27	4.3	CVE-2013-4664 MISC MISC MISC
support_incident_tracker_project -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the search_id parameter in the search_incidents_advanced.php page is affected by XSS.	2020-01-02	4.3	CVE-2019-20220 MISC
support_incident_tracker_project -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Short Application Name and Application Name inputs in the config.php page are affected by XSS.	2020-01-02	4.3	CVE-2019-20222 MISC
support_incident_tracker_project -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, Load Plugins input in the config.php page is affected by XSS. The XSS payload is, for example, executed on the about.php page.	2020-01-02	4.3	CVE-2019-20221 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
support_incident_tracker_project -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the id parameter is affected by XSS on all endpoints that use this parameter, a related issue to CVE-2012-2235.	2020-01-02	4.3	CVE-2019-20223 MISC
tbeu -- matio	A stack-based buffer over-read was discovered in ReadNextCell in mat5.c in matio 1.5.17.	2019-12-27	4.3	CVE-2019-20018 MISC
tbeu -- matio	A stack-based buffer over-read was discovered in Mat_VarReadNextInfo5 in mat5.c in matio 1.5.17.	2019-12-27	4.3	CVE-2019-20017 MISC
tbeu -- matio	A stack-based buffer over-read was discovered in ReadNextStructField in mat5.c in matio 1.5.17.	2019-12-27	4.3	CVE-2019-20020 MISC
tbeu -- matio	An attempted excessive memory allocation was discovered in Mat_VarRead5 in mat5.c in matio 1.5.17.	2019-12-27	4.3	CVE-2019-20019 MISC
toshiba -- configfree	Multiple stack-based buffer overflows in CFProfile.exe in Toshiba ConfigFree Utility 8.0.38 allow user-assisted attackers to execute arbitrary code.	2019-12-27	6.8	CVE-2012-4980 BID XF
upx -- upx	A heap-based buffer over-read was discovered in canUnpack in p_mach.cpp in UPX 3.95 via a crafted Mach-O file.	2019-12-27	4.3	CVE-2019-20021 MISC
winamp -- winamp	Winamp 5.63: Invalid Pointer Dereference leading to Arbitrary Code Execution	2019-12-27	6.8	CVE-2013-4695 MISC MISC
wordpress -- wordpress	WordPress Xorbin Digital Flash Clock 1.0 has XSS	2019-12-27	4.3	CVE-2013-4693 MISC
wordpress -- wordpress	WordPress before 5.3.1 allowed an attacker to create a cross-site scripting attack (XSS) in well crafted links, because of an insufficient protection mechanism in wp_targeted_link_rel in wp-includes/formatting.php.	2019-12-27	4.3	CVE-2019-20042 MISC MISC MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	An XSS issue was discovered in the Laborator Neon theme 2.0 for WordPress via the data/autosuggest-remote.php q parameter.	2019-12-30	4.3	CVE-2019-20141 MISC
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in the Conversador plugin 2.61 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the 'page' parameter.	2019-12-27	4.3	CVE-2014-4519 MISC
wordpress -- wordpress	WordPress before 5.3.1 allowed an unauthenticated user to make a post sticky through the REST API because of missing access control in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php.	2019-12-27	5	CVE-2019-20043 MISC MISC MISC MISC
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in rss.class/scripts/magpie_debug.php in the WP-Planet plugin 0.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-12-27	4.3	CVE-2014-4592 MISC
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in the Easy Career Openings plugin 0.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2019-12-27	4.3	CVE-2014-4523 MISC
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php in the Ebay Feeds for WordPress plugin 1.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the rss_url parameter.	2019-12-27	4.3	CVE-2014-4525 MISC CONFIRM
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in preview-shortcode-external.php in the Shortcode Ninja plugin 1.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the shortcode parameter.	2019-12-27	4.3	CVE-2014-4550 MISC
xnview -- xnview	Stack-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted image layer in an XCF file.	2020-01-02	6.8	CVE-2013-3246 MISC MISC
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted RLE compressed layer in an XCF file.	2020-01-02	6.8	CVE-2013-3247 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 168924.	2019-12-30	3.5	CVE-2019-4623 XF CONFIRM
ibm -- watson_studio_local	IBM Watson Studio Local 1.2.3 stores key files in the user's home directory which could be obtained by another local user. IBM X-Force ID: 161413.	2019-12-30	2.1	CVE-2019-4335 XF CONFIRM
nagios -- nagios_xi	In Nagios XI 5.6.9, XSS exists via the nocscreenapi.php host, hostgroup, or servicegroup parameter, or the schedulereport.php hour or frequency parameter. Any authenticated user can attack the admin user.	2019-12-30	3.5	CVE-2019-20139 MISC
tenable -- nessus	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would only potentially impact other admins. (Tenable ID 5198).	2019-12-27	3.5	CVE-2016-1000028 MISC MISC CONFIRM
tenable -- nessus	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would potentially impact other admins (Tenable IDs 5218 and 5269).	2019-12-27	3.5	CVE-2016-1000029 MISC MISC MIS